Secure Certificate and System and Method for Issuing and Using Same

(A-70559/RMA)

WE CLAIM:

1. A computer program product for use in conjunction with a computer system having a server and a client, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism, comprising: a program module that directs the computer system and/or components thereof including at least one or the client or server, to function in a specified manner to provide message communications, the message communications occurring in a computer system hardware architecture neutral and operating system neutral and network transport protocol neutral manner for secure certificate issuing by an Issuer to a Client requesting the certificate, the program module including instructions for:

A. extracting, by a certificate requesting client, a network address for the Issuer from a trusted source or storage means;

B. extracting, by the client, a Resource Tag related to its own Subject Name from a message that was received from a Server;

C. extracting, by the client, a public and private key and certificate chain from a trusted source;

D. using the extracted information to create a secure session with the Issuer that authenticates the issuer using the same protocol;

E. sending, by the client, as the client's first Data message after any session setup messages, a data structure that has a common header with fields for Type, Version and Content-Length, and contents that include the Resource Tag, the Client's Subject Name, and optionally one or more public keys that the Client has generated;

F. verifying, by the certificate issuer, that a valid Server issued the Resource Tag and that the Resource Tag is valid for the given received Subject Name;

G. creating, by the issuer, a Compact Certificate with one or more public keys and with the Client's Subject Name;

H. digitally signing, by the issuer, the certificate with the Issuer's private key; and

I. sending, by the certificate issuer, a message back to the Client over the secure channel, where the message includes the Compact Certificate and if the Issuer generated the public key(s), the message includes the matching private key(s).

2. A hardware architecture neutral and operating system neutral and network transport neutral method for secure certificate issuing by an Issuer to a Client requesting the certificate using less software code and network bandwidth than conventional systems, said method comprising the steps of:

A. extracting, by a certificate requesting client, a network address for the Issuer from a trusted source or storage means;

B. extracting, by the client, a Resource Tag related to its own Subject Name from a message that was received from a Server;

C. extracting, by the client, a public and private key and certificate chain from a trusted source;

D. using the extracted information to create a secure session with the Issuer that authenticates the issuer using the same protocol;

E. sending, by the client, as the client's first Data message after any session setup messages, a data structure that has a common header with fields for Type, Version and Content-Length, and contents that include the Resource Tag, the Client's Subject Name, and optionally one or more public keys that the Client has generated;

F. verifying, by the certificate issuer, that a valid Server issued the Resource Tag and that the Resource Tag is valid for the given received Subject Name;

G. creating, by the issuer, a Compact Certificate with one or more public keys and with the Client's Subject Name;

H. digitally signing, by the issuer, the certificate with the Issuer's private key; and

I. sending, by the certificate issuer, a message back to the Client over the secure channel, where the message includes the Compact Certificate and if the Issuer generated the public key(s), the message includes the matching private key(s).

3. The method in Claim 2, further comprising: the client placing the Compact Certificate and keys into its trusted source or storage means.

4. The method in Claim 2, wherein the one or more public key(s) are generated by the Issuer or send to the Issuer by the Client who generated them.

5. The method in Claim 2, wherein where the one or more public key(s) are sent to the Issuer by the Client who generated them.

6. The method in Claim 2, wherein the trusted source or storage means is data compiled into the Client software.

7. The method in Claim 2, wherein the trusted source or storage means is data received from communicating with a Server via a secure session.

8. The method in Claim 2, wherein the trusted source comprises a trusted storage.

9. The method in Claim 2, wherein the network address comprises a URL.

10. The method in Claim 2, wherein the Resource Tag comprises a message tag.

11. The method in Claim 2, wherein the Subject Name comprises an e-mail address.

12. The method in Claim 2, wherein the public and private key operations are performed by any asymmetric cryptosystems.

13. The method in Claim 12, wherein the asymmetric cryptosystem is selected from the group consisting of RSA, Elliptic Curve, and NTRU.

14. The method in Claim 2, wherein the public and private key extracted by the client are fixed public and private keys.

15. The method in Claim 2, wherein the public and private key and certificate chain extracted by the client are fixed public and private keys and certificate chain.

16. A method for secure certificate issuing by an issuer to an entity requesting the certificate, said method comprising:

extracting, by the entity, a network address for the certificate issuer from a trusted source;

extracting, by the entity, information including a resource tag related to its own subject name from a message that was received from a server, and a public key and a private key and certificate chain from a trusted source;

using, by the entity, the extracted information to create a secure session with the issuer that authenticates the issuer; and

sending, by the entity, as a component of the entity's first data message after any session setup messages, a data structure that includes the resource tag and subject name.

17. The method of claim 16, further comprising:

verifying, by the issuer, that a valid server issued the resource tag and that the resource tag is valid for the given received subject name;

creating, by the issuer, a certificate with one or more public keys and with the entity's subject name;

digitally signing, by the issuer, the certificate with the issuer's private key; and

sending, by the issuer, a message back to the entity over the secure channel, where the message includes the certificate.

18. The method of claim 17, further comprising: receiving the certificate by the requesting entity.

19. The method of claim 17, wherein the requesting entity comprises a requesting client.

20. The method of claim 16, wherein the requesting entity comprises a requesting client.

21. The method of claim 17, wherein if the issuer generated the public key(s), the message sent back to the entity includes the matching private key(s).

22. The method of claim 17, wherein the requesting entity comprises a requesting client.

23. The method of claim 17, wherein the data structure includes a common header with fields for type, version, and content-length, and contents that include the resource tag, the entity's subject name.

24. The method of claim 23, wherein the data structure further optionally includes one or more public keys that the entity has generated.

25. The method of claim 24, wherein the entity comprises a client.

26. The method of claim 2, wherein the trusted source or storage means comprises a Compact Certificate as explained earlier, or chain of Compact Certificates leading to a trusted root public key.